IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA *v.* FARAMARZ SHAHI SAVANDI AND MOHAMMED MEHDI SHAH MANSOURI	Criminal Indictment No. 1:18CR473

THE GRAND JURY CHARGES THAT:

Introduction

1. On or about March 10, 2018 through on or about March 22, 2018, the defendants, FARAMARZ SHAHI SAVANDI and MOHAMMED MEHDI SHAH MANSOURI, both of whom are Iranian nationals, caused the execution of a "ransomware" attack against the City of Atlanta, which encrypted vital City of Atlanta computer systems, and demanded a ransom payment to restore access.

2. The attack was executed by the use of a type of malware (or "ransomware") referred to as "SamSam Ransomware," which infected approximately 3,789 computers belonging to the City of Atlanta, including servers and workstations. Once deployed, the ransomware encrypted the files associated with each infected computer and displayed a ransom note. That is, the ransomware effectively locked the infected computers and made it impossible to access the information stored on them without a decryption key.

3. The ransom note demanded .8 Bitcoin[1] to decrypt each affected computer or 6 Bitcoin to decrypt all affected computers. That is, the attackers gave the City of Atlanta the option of paying to decrypt certain computers (at a rate of .8 Bitcoin per computer) or to decrypt all the infected computers (for 6 Bitcoin). The ransom note directed the City of Atlanta to a particular Bitcoin address[2] to pay the ransom and supplied a web domain that could only be accessed using a TOR browser; the note suggested that the City of Atlanta could download the decryption key from that website. But, in the days following the attack, the webpage that purportedly contained the decryption key became inaccessible, and the City of Atlanta did not pay the ransom.

4. The attack significantly disrupted City of Atlanta operations, impaired certain governmental functions, and caused it to incur significant expenses in the coming weeks and months.

---

[1] Bitcoin is a decentralized digital currency that may be used to purchase goods and services online, or traded on online exchanges for conventional currencies, including the U.S. dollar and the Euro.

[2] A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password or PIN needed to access the address. Only the holder of an address's private key can authorize any transfers of Bitcoin from that address to other Bitcoin addresses.

Count 1

(Computer Fraud and Abuse: Intentionally Causing Damage)
(18 U.S.C. § 1030(a)(5)(A))

5. On or about March 10, 2018 through on or about March 22, 2018, in the Northern District of Georgia and elsewhere, the defendants, FARAMARZ SHAHI SAVANDI and MOHAMMED MEHDI SHAH MANSOURI, aided and abetted by each other, knowingly caused the transmission of a program, information, code, and command, that is, "SamSam Ransomware," and as a result of such conduct, intentionally caused damage without authorization to a protected computer with the offense loss aggregating at least $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer and a threat to public health and safety, and damage affecting at least ten protected computers during a one-year period.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), 1030(c)(4)(B) and Section 2.

A True BILL

FOREPERSON

BYUNG J. PAK
United States Attorney

NATHAN P. KITCHENS
Assistant United States Attorney
Georgia Bar No. 263930

KAMAL GHALI
Assistant United States Attorney
Georgia Bar No. 805055

600 U.S. Courthouse
75 Ted Turner Drive SW
Atlanta, GA 30303